COMPAQ

Database Technology and Solutions Center

DTSC WHITE PAPER

Compaq 9th Annual Systems Engineering Conference – Living LAB

ECG05/0998 August, 1998

CONTENTS

Oracle Fail Safe 2.0 Performance on Compaq ProLiant Servers

ABSTRACT

Oracle Fail Safe(OFS) on Compaq servers has been one of the most reliable and mature high availability solution on Microsoft Windows NT MSCS. Compaq's Database Technology and Solutions Center(DTSC) has conducted a series of performance tests to characterize the performance of Oracle Fail Safe running on Compaq ProLiant servers. The tests also captured the impact of system loads as additional processors were added to the test systems.

These tests were performed at the Compaq/Oracle International Competency Center (ICC), located within the Compaq DTSC in San Bruno, California. The Compaq/Oracle ICC was established to address Oracle database related issues such as solution development and validation, advanced technology, customer case studies and proof of concept projects.

The main focus of the tests were to,

- Evaluate the system performance in the two node fail over environment
- Capture the fail over performance of the system under various user loads
- Characterize the performance of the surviving node as well as the failing node when using one, two, or four processors on both servers

The test results indicated,

- The overall performance in the OFS environment is highly dependent on the system load of each server.
- When the combined system load on the surviving node and the failing node was under 90%, the performance of the surviving node is similar to the baseline tests. The baseline tests were implemented to measure the performance of each server without the fail over event.
- When the combined loads were over 90%, the fail over performance and the performance of the surviving node degraded compared to the performance of the baseline tests.
- When the surviving node was heavily loaded, adding additional processors to the node helped to improve the overall system performance.

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirement. Compaq does not warrant products other than it's own as stated in product warranties.

PREPARED BY
Compaq Database Technology and Solutions Center
Client/Server Solutions, INC
Oracle Corporation

INTRODUCTION

There are three demonstrations designed for the SE conference living lab session.

Living Lab Demonstrations

Demo #1: OFS overview/simple transaction fail over

This demo illustrates a basic setup of the OFS environment on Compaq servers, and how a simple query reacts when the database server fails.

Demo #2: Automatically client re-connect implementation

Through a sample C program, it shows how the application program uses Oracle Call Interface(OCI) to implement the re-connect feature.

Demo #3: OFS Performance characterization

This demo illustrates the OFS performance under various number of users and system load.

OFS Overview

Oracle Fail Safe is the easy-to-use high availability option for Oracle databases.

- Oracle® Fail Safe databases are highly available with fast automatic failover capabilities. Oracle Fail Safe server optimizes instance recovery time for Oracle Fail Safe databases during planned and unplanned outages.
- Oracle Fail Safe configuration and management is straightforward with Oracle Fail Safe Manager, the easy-to-use graphical user interface (GUI). This is integrated with Oracle® Enterprise Manager for comprehensive database administration.
- Oracle Fail Safe databases are configured within *virtual servers* that allow client applications to access Oracle Fail Safe databases at a given network name at all times, regardless of the cluster node hosting the database.

There are three major ways to deploy the OFS solutions.

1. Standby (Active/Passive)

The 'standby' solution is expensive since it requires one additional server standing by to take over the existing server in the event of failure. The 'standby' solution will be able to provide the best response time since the backup server is idle all the time.

2. Active/Active

The 'active/active' solution may be the most commonly used solution since both servers can be utilized at all times. Meanwhile they are both configured to back each other up in the event of failure.

3. Partitioned Workload

The 'partitioned workload' is a variation of 'active/active' solution. The only difference is that one server is setup as an application server where the other is a database server.

Appendix B addresses answers to some of the frequently asked questions of OFS, and the document was down-loaded from the Oracle web site, http://www.oracle.com/.

Scope

The major intent of this tech note is to share the findings of the performance characterization tests using the 'active/active' solution on Compaq servers. All tests were performed in a controlled laboratory environment. The goal was to establish a consistent test bed where all the test results can be compared fairly. Therefore, the test environment was not tuned for optimal performance. The demo environment used at the 9th ASE conference is a smaller scale of environment in the lab.

TEST APPROACH

Test Environment

Hardware

Model (Quantity)	Usage	# CPU	RAM	Miscellaneous
ProLiant Servers (2)	Database Server	2 P6	1GB	1 Fiber card; 2 network card
DeskPro (2+)	Database Clients	1 P6	128MB	
Fiber hub (1)				
Fiber storage (1)	Shared storage			13 4.3GB drives
Network hub (1)				

Software

Database Server 1	**Database Server 2**	**Database Clients**
- Windows NT 4.0 MSCS - Oracle 8.0.4; OFS 2.0 - Complex OLTP workload; - DB Size: ~8GB	- Windows NT 4.0 MSCS - Oracle 8.0.4; OFS 2.0 - AS3AP database - DB Size: ~16GB	- Windows NT 4.0

The overall test environment is illustrated as Figure 1 in the next page. **Appendix A** documented 14 steps for building a two-node OFS environment.

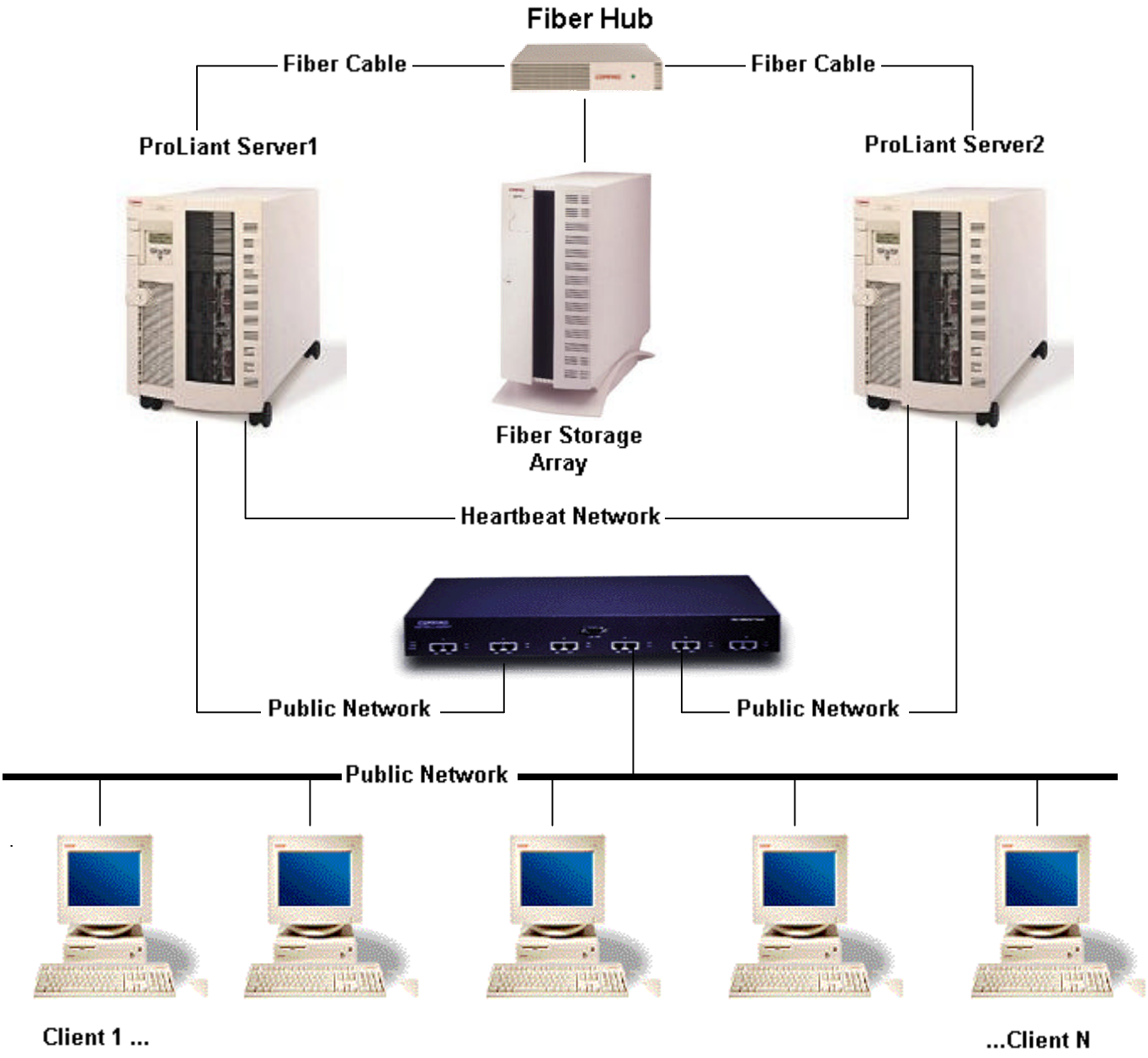


Figure 1: Two-Node OFS environment layout

Test Methodology

Benchmark Factory 97 was the tool used to build the workloads on both database servers. The tool also provided the capability of simulating users from the client system in the test environment, displaying real time statistics, and collecting the test statistics for the tests.

Benchmark Factory Overview

Benchmark Factory (BF) has two main components. The first component is the Visual Control Center (VCC); used to prepare, execute and evaluate the tests performed by Benchmark Factory. The VCC module also holds the data repository where all the test results are kept for future analysis. The other component is the Agent. This module can either be installed on the same machine as the VCC or on one or more other machines. The agent allows many users to login to the Server Under Test (SUT) from any given client machine. In a typical test, you would have many agents, each running on their own client machine, and one VCC running on its own machine.

Visual Control Center

The Visual Control center (VCC) is the main component of Benchmark Factory 97. From here, you are able to set up all of your tests as well as populate your test databases. You can also control the other component of the product, the Agent, from the VCC and watch the statistics of the actual tests being performed in real time.

The Agent

The agent is the workhorse of the Benchmark Factory product. It is the application that resides on the machines that are to be used as the client machines for the tests. This agent is installed from a special directory created during the installation of the VCC. . Installation from this directory makes the setup of the agent on a large number of machines a very quick and simple task. Once the agent is installed on the client machine, it automatically attempts to connect up with the VCC and is instantly ready to perform a test. The agent gets all its instructions from the VCC, making it very simple to control hundreds of machines running the agent module from a single location.

Detail product information can be found on http://www.benchmarkfactory.com/.

Client re-connect implementation

To fail over a database transaction requires special implementation. The application program needs to take most of the responsibility to handle the return code from the database server and to make the appropriate response. Oracle 8 Server on NT supplies interfaces, Oracle Call Interface (OCI) , for the database application to handle the fail over condition. It provides calls for applications to be able to connect back to the database instance, after the instance fails from one server to another. It also provides the ability for resuming the position and continuing the fetch operation after the fail over completes. In the event of INSERT, UPDATE, or DELETE situations, it will be the responsibility of the application program to verify if the transaction had been committed before fail over occurred using the return code from the OCI calls. The application then determines if the transaction needs to be re-issued after reconnecting to the database instance.

TEST FINDINGS

-Overall performance was reasonably well

The overall performance in the OFS environment was good when both the failing node and the surviving node had a light or medium system load at the time the fail over occurred.

-System load impacts performance

We experienced performance degradation when the system load on the surviving node became very high after taking over all the work from the failing node.

-Additional processors relieve system load

Adding additional processors to the surviving node relieved the system load especially when the majority of the work was CPU bound.

-Automatically client reconnect

The read-only transactions were handled by Oracle Call Interface (OCI). When the fail over occurred, all users on the failing node can be re-connected to the surviving node automatically if the application program is implemented properly. The read-only transaction could also be resumed after it was re-connected to the surviving node.

-Reasonable time to re-connect clients

When one node failed, the time to reconnect the clients from the failing node to the surviving node is dependent to the system load and the number of users.

When both system loads were light or medium, each user on the failing node took 40 to 60 seconds to reconnect to the surviving node. If the combined system load was over 90%, it took from 1 to 2 minutes.

The number of users required to reconnect to the surviving node also impacted the reconnect time. Comparing the reconnection of 20-user vs. 40-user cases, the average time to reconnect each user in the 40-user case was 15% longer than the 20-user case.

-Longer execution time for transactions experiencing fail-over

The database transactions running on the surviving node experienced very little impact when the system was not heavily loaded after the fail over occurred.

The database transactions running on the failing node took at least 1 minute longer to complete when the fail over occurred. The additional time was used to reconnect the user to the surviving node. It took longer when the surviving node was heavily loaded. After the user was reconnected to the surviving, it resumed processing the transaction.

The details of the test results is documented in the DTSC Lab Report, which will be available on Compaq web site in the near future.

Appendix A

Installation and Configuration of Oracle Fail Safe 2.1 on Compaq ProLiant Servers for the 9th ASE Conference

This document outlines the fourteen steps required to setup a two-node OFS system. These steps built the environment below with the two servers being able to back each other up in the event of system failure.

- Two ProLiant Servers
- Two Client System
- One Shared Fiber Storage System

The document assumes that readers are knowledgeable about Compaq, Oracle Server on NT, Microsoft Windows NT, and Microsoft Cluster Server Products.

Before step 1, ensure all physical connections between the servers, clients, the fiber storage, and network links are all properly connected.

Compaq High Availability web site will have the following document available for a detail description of installation and configuration of OFS on Compaq Servers. The document is titled, 'Implementing Oracle Failsafe 2.1.2 and Microsoft Cluster Server on Compaq ProLiant Clusters'.

STEP 1: Update all firmware for both nodes to their current versions.

- ❑ ProLiant Firmware. (We used version 04/29/98)
- ❑ Fiber Channel Storage Array Subsystem Firmware.
- ❑ Fibre Adapter Cards and Connectors.
- ❑ Smart2 Controller
- ❑ Hard drives

STEP 2: Run the Compaq SmartStart CD to both nodes. (version 4.0)

- ❑ Run the system eraser utility.
- ❑ Run the system configuration utility.
- ❑ Set all cards to their appropriate IRQ setting. See the Hardware Configuration layout in the Appendix.
- ❑ Use the ACU utility to partition the shared storage to its appropriate RAID level and Logical Drives.
- ❑ Create a Compaq partition on the local drive.

STEP 3: Install Windows NT on both nodes. (We used NT 4.0 Enterprise Edition)

Note: Microsoft Cluster Server requires that all computers in the cluster belong to the same domain. Login for each node requires that both nodes have the same username, password, and administrator privileges. The following steps were performed for our demo setup configuration. If you are installing a cluster into an existing domain environment, it is not required to setup a PDC or BDC.

- ❑ Install server1 (node1) as the Primary Domain Controller (PDC).
- ❑ Install server2 (node2) as the Backup Domain Controller (BDC).
- ❑ Set virtual memory = 500MB (This step is optional).
- ❑ Set the foreground and background application as equal.
- ❑ From the Control Panel➔Network➔Services➔Server➔Property and select "Maximize throughput for network applications". (This step is optional.)
- ❑ If the Installer brings up the nhloader, exit this screen. This will be used later to install MSCS.

STEP 4: Install Service Pack 3 (SP3) to both nodes.

- ❑ Select "Yes" to overwrite the "cpqflxe.sys" file.
- ❑ Reboot both the machines.

Note: After installing SP3 to both nodes, use the Disk Administrator to verify all default partitions and all drive letters from server1 are the same as server2. We used drive C for system and Oracle files and drive D for the CD ROM.

STEP 5: Run Compaq NTSSD from the SmartStart CD to all required nodes.

- ❑ Go to \cpqsupportsw\ntssd and run setup.exe.
- ❑ Select "Express setup" unless there are overhead issues, in which case only load the support drivers for Fibre Channel, Network Card, SCSI, and Smart2 card.
- ❑ Invoke NT Disk Administrator to create all required partitions on the shared storage. All drive letters from server1 must be the same on server2. We used drive C=system files and Oracle files, drive D=CD ROM, drives E, F, and G as the shared disks.
- ❑ Reboot the machines.

Note: If you have NT Service Pack 4 (SP4), the Compaq Fibre Channel Storage Driver is located in \Drivlibs\storage\cpqcalm\i386 directory.

STEP 6: Create Windows NT hosts and lmhosts files for the entire cluster.

Note: Lmhosts file is not needed if the cluster is within the same subnet as all the clients. When modifying the lmhosts file from the DOS prompt, refresh the cache with the commands Nbstat-R and Nbstat-c.

- ❑ Locate the hosts and lmhosts files in \winnt\system32\drivers\etc on server1.
- ❑ Add the computer's name and the public communication's IP to the hosts and lmhosts files for all nodes and clients which participate in the cluster. (Failsafe requires that the hosts file includes the computer's name and IP.)

STEP 7: Check and Test the IP bindings for all required nodes.

- ❑ At the dos prompt on each node, ping the computer's name to verify that the return IP address is correct for "public communication". If the IP address is incorrect, correct the IP address for the network card.

STEP 8: Install Microsoft Cluster Server 1.0 (MSCS) on both nodes.

- ❑ Click on "Start" ➔ "Run" and at the "Open" box type in "nhloader" and <enter>.
- ❑ Select "Continue" to continue the installation.
- ❑ Select "Microsoft Cluster Server" and "Start Installation".
- ❑ When prompted, insert disk 2 of Windows NT 4.0 Enterprise Edition in the CD-ROM drive and click "OK" to continue.
- ❑ At the "Microsoft Cluster Server Setup" screen select "Next" to continue, "I Agree", then "Next".
- ❑ Select one of the following three options:
  a) Form a new cluster – select if this is the first cluster installation in the configuration. Use this option for the first server.
  b) Join an existing cluster – select if a server is joining a cluster that already exists. Use this option for the second server. (You will see less steps in the installation for this option.)
  c) Install Cluster Administrator only – select if the Cluster Administrator console, used to monitor the cluster, is to be installed on a computer system.
- ❑ Enter the name for the cluster being formed or joined, then click "Next".
- ❑ Click "Next" for "Setup will place the cluster files in this folder".
- ❑ Add all available unshared disks to the right side as shared cluster disks, then click "Next".
- ❑ "Select the shared disk on which to store permanent cluster files" screen allows you to select the Quorum drive. The Quorum drive contains the cluster files, keeping MSCS alive. Select a "shared" disk or use the default, then click "Next" twice.
- ❑ Enter the "Network Name" that will be used for network communication, and enable the network to be used by the cluster as:
  a) Use for all communications – select if this network is to be used for all private and public communications.
  b) Use only for internal cluster communications – select if the network is only used for the "heartbeat" or private communication between the two cluster nodes.
  c) Use only for client access – select if the network is only used for client or public communication.
- ❑ Click "Next", enter the IP address and subnet mask for the cluster, then click "Next" again.
- ❑ Click "Finish" to copy the files, then reboot the nodes.

STEP 9: Install Oracle on both nodes. (We used v.8.0.4. Apply any necessary patches after the installation.)

Note: For additional help, refer to Oracle installation documentation.

- ❑ Place the Oracle CD in the CD-ROM drive of the primary server, server1.
- ❑ When the installation screen appears, click on "Begin Installation".
- ❑ At the "Oracle Installation Settings" screen, the following should appear for the Oracle Home:
- ❑ Name =DEFAULT_HOME
- ❑ Location =C:\ORANT
- ❑ Language =ENGLISH
- ❑ Click "OK" if the above is correct.
- ❑ Select "Oracle8 Enterprise Edition" as the installation option, then click "OK".
- ❑ Select Cartridges and Options if purchased, else click "OK". (This document does not support options.)
- ❑ At "Select a Starter Database Configuration" screen, select "None" and "OK". (Select "Typical Configuration" if you want a sample database to automatically be created during the installation.)
- ❑ Select "Yes" if you want to install Legato Backup Manager at the "Installation Legato Storage Manager" screen, else click "NO".
- ❑ Select whether to install Oracle Online Documentation, which requires 75MB of hard disk space.
- ❑ Click "OK" at the "Reboot Needed" screen, close all open windows and reboot the system.
- ❑ After reboot, confirm that the following services are started by using the "Services" utility in the "Control Panel":
- ❑ OracleAgent80----------started
- ❑ OracleTNSListener80------started
- ❑ OracleWebAssistant80-----started
- ❑ If any of the above services are not started, highlight the service and click on the "Start" button located on the right side of the screen.

STEP 10: Update both nodes with the latest patch for Oracle. (We used v.8.0.4.1.3)

- Stop OracleTNSListener80 and OracleWebAssistant80 services before installing the patch.
- Run the setup.exe and install the patch.

STEP 11: Install Oracle Fail Safe for Oracle8 and Fail Safe Manager to both nodes.

Note: Ensure that all required patches are installed. Verify that the Microsoft Cluster server and both nodes are up and running prior to installing Fail Safe.

- Place the Oracle Fail Safe CD in the CD-ROM drive and click "Begin Installation".
- Verify that the "Oracle Installation Settings" are the same as in Step 9, then click "OK".
- Click "Install" at the screen where Oracle Fail Safe Server and Oracle Fail Safe Manager are highlighted.
- Select "Install the Fail Safe Documentation and Quick Tour".
- Select "Yes" to "Install Oracle Intelligent Agent 8.0.4.1.2".
- Reboot the machines.

STEP 12: Create the Fail Safe Group (Virtual Server).

- Login to the Fail Safe Manager on server1.
- Select "Yes" when asked if you want to verify the cluster.
- Click "OK" if you see a message stating that it could not see the standalone databases. (This requires that the Oracle Enterprise Manager be up and running, this step will be performed later.)
- From the Fail Safe Manager, click on "Fail Safe Groups" and select "Add".
- Enter the Group name. This will be an alias in the Microsoft Cluster Administrator for the resource group that is automatically created.
- Select "Networks accessible by clients" and enter "client connection" for the network to use, the network name, IP address, and the subnet mask.
- Specify the "Failover Period" and "Failover Threshold", then click "Next".
- Select a "Preferred Node" for the failback, else click "next".
- Click "OK" to confirm, and repeat the above steps for server2.
- Verify the Fail Safe group and cluster by selecting the "verify group" and "verify cluster" options from the Fail Safe Manager menu. If either fails, delete and rebuild them.

STEP 13: Create a Standalone Database.

A standalone database is a database that does not belong to the Fail Safe Group. When a database already exists or is created, it is a standalone database until it is moved to a Fail Safe Group, then it becomes a Fail Safe Database. A sample database can be created using the Fail Safe Manager. When creating a custom database, place the database on the shared disk and verify the database using the "verify standalone database" option from the Fail Safe Manager menu.

STEP 14: Add the Standalone Database to the Fail Safe Group.

If a standalone database is on the shared disk, but does not display as a GUI, use the Fail Safe Manager menu option "verify standalone database". After the verification is successful, add the standalone database to the Fail Safe Group by selecting "Add database to Fail Safe group" from the Fail Safe Manager menu.

INSTALLATION TIPS

- **Change Oracle Default Password**

Some of the Oracle "create database" scripts use "internal/oracle" or "internal/manager" as the password. To change the default password to suit your needs, use the orapwd80.exe utility located in the Orant\bin directory.

- **Tnsname.ora**

In the tnsname.ora file, modify the host name to the name of the virtual computer used by the clients. Use the Fail Safe "aware" tnsname.ora file, which can be found on the Oracle Fail Safe CD, instead of the default tnsname.ora file.

- **Windows NT Server Network Binding Order**

When two network cards are in a system, Windows NT should bind the IP address to the cards according to the order in which they are specified in Control Panel→Network→TCP/IP→Property. To ensure that the order is correct, before installing Microsoft Cluster Server, check and test the binding order of the cards. To do this, at the DOS prompt ping the computer names for the nodes being used for public communication or client access. You should see the network IP binding for the card used for public communication. If you see the IP binding for the heartbeat or private communication, switch the IP addresses on the network cards.

- **Remote Procedure Call (RPC) Locator Error for MSCS**

Sometimes when opening Microsoft Cluster Administrator, an error message indicating that there is a problem with RPC may appear. Go to Control Panel→Services and stop the RPC locator and restart it again. A fix for this problem is available from the Microsoft Web site, see cluster setup.

- **Fiber Channel Storage Host Adapter Driver**

If you have the Microsoft Windows NT Service Pack 4 (SP4) CD, the Compaq Fiber Channel Storage Host Adapter Driver is located in the \Drvlibs\storage\cpqcalm\i386 directory.

- **Recovery From a System Crash**

After a crash, move the database to the surviving node, then reload Microsoft Windows NT 4.0, Service Pack 3, MCSC, Oracle 8.0.4, and Fail Safe 2.1.x onto the crashed system.

Move the crashed system's database from the "Fail Safe group" to a "standalone database". Now, add this standalone database back to the Fail Safe group. This process will automatically reload the instances on both nodes.

- **Create or Add a Tablespace in the Fail Safe Environment**

When creating or adding a tablespace, remember to put the data files on the desired shared disk. Verify the group by using the Fail Safe Manager.

- **Create a Custom Database**

Use Oracle Database Assistant to create a typical or custom database, locating the parameter, log, data, init, trace, control, and redo log files onto the shared storage array drives.

- **Performance and Capacity Considerations**

Create or use a simulator application tool to simulate the number of users, workload, and type of applications being used, before actually deploying your configuration into a production environment.

Appendix B (Prepared by Oracle Corporation)

Oracle® Fail Safe 2.1

Frequently Asked Questions

ORACLE®

Oracle Fail Safe

What is Oracle Fail Safe?

Oracle Fail Safe is the easy-to-use high availability option for Oracle databases.

- Oracle® Fail Safe databases are highly available with fast automatic failover capabilities. Oracle Fail Safe server optimizes instance recovery time for Oracle Fail Safe databases during planned and unplanned outages.
- Oracle Fail Safe configuration and management is straightforward with Oracle Fail Safe Manager, the easy-to-use graphical user interface (GUI). This is integrated with Oracle® Enterprise Manager for comprehensive database administration.
- Oracle Fail Safe databases are configured within *virtual servers* that allow client applications to access Oracle Fail Safe databases at a given network name at all times, regardless of the cluster node hosting the database.

How do Oracle Fail Safe and Oracle Parallel Server compare?

Oracle Fail Safe	Oracle Parallel Server
Targets departmental and workgroup customers seeking highly available Windows NT cluster solutions.	Targets enterprise-level and corporate customers seeking highly available and scalable cluster solutions.
Provides highly available single-instance databases.	Provides scalable, highly available multi-instance parallel databases.
Windows NT only solution.	Available on all major platforms.
Tuning and other management operations are the same as for a single-instance Oracle database.	Tuning and other management operations require multi-instance Oracle database and cluster configuration knowledge.
Maximum of 2 nodes in a cluster; current limitation is required by underlying Microsoft Cluster Server.	Supports more than 2 nodes in a cluster; does not use Microsoft Cluster Server software.

How do the Oracle Fail Safe releases differ?

- Oracle Fail Safe 2.1 supports both Oracle7™ and Oracle8™ databases.
- Oracle Fail Safe 2.0 supports only Oracle7 databases.
- Oracle Fail Safe 2.0 and 2.1 provide a software-only solution for Windows NT clusters layered over Microsoft Cluster Server, and feature Oracle Fail Safe Manager to configure groups, set conditions, and optimize failover and failback of Oracle databases.
- Oracle Fail Safe 1.0 and Oracle Fail Safe 1.1 are earlier custom hardware-based solutions that are specific to Compaq ProLiant servers and require the Compaq Online Recovery Server.

What network protocols and disk formats does Oracle Fail Safe Release 2.1 support on Windows NT?

- TCP/IP network protocol
- NTFS formatted disks on a shared storage interconnect for the Oracle Fail Safe database files

Oracle Fail Safe Manager

What is Oracle Fail Safe Manager?

Oracle Fail Safe Manager is a configuration and management GUI that includes wizards, drag-and-drop capabilities, online help, and tutorials to:

- Configure standalone Oracle databases into Oracle Fail Safe databases
- Manage Oracle Fail Safe databases in clusters
- Monitor, verify, and help to load balance Oracle Fail Safe databases

When do I use Oracle Fail Safe Manager and Oracle Enterprise Manager tools?

- Use Oracle Fail Safe Manager for cluster-related configuration and management operations of Oracle Fail Safe databases.
- Use Oracle Enterprise Manager for routine database administration tasks (such as database backup and restore operations, or SGA analysis) of Oracle Fail Safe databases.

How does Oracle Fail Safe Manager differ from Microsoft Cluster Administrator?

- Oracle Fail Safe Manager and Oracle Fail Safe server have built-in knowledge of Oracle databases and their operation on Windows NT clusters.
- Microsoft Cluster Administrator is not adequate for configuration and management of Oracle databases.

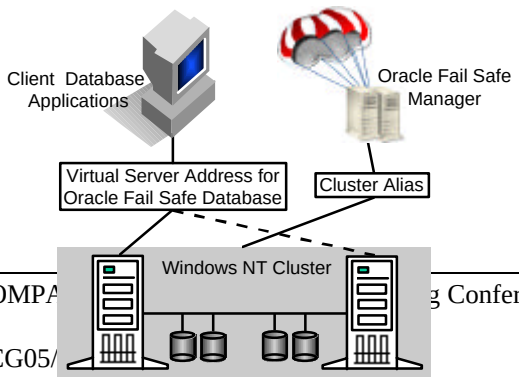
Client Applications

What changes do I need to make on the client to access an Oracle Fail Safe database?

- No changes are required to the application code.
- On the client system, the virtual server address for the Oracle Fail Safe database has to be registered.

Do my applications connect using the cluster alias?

- No. The cluster alias is used only for cluster administration purposes by Microsoft Cluster Administrator and Oracle Fail Safe Manager, as shown in the figure below.



- Applications connect to the Oracle Fail Safe database using the virtual server address.

How does a failover affect database applications?

- The failover appears as a brief network outage.
- Client applications simply reconnect using the virtual server address and continue processing transactions against the Oracle Fail Safe database.

Failover Timing

What are typical failover times?Oracle Fail Safe server optimizes the time it takes to fail over an Oracle Fail Safe database. Failover times vary and depend on the following three parameters:

- Workload on the Fail Safe database server
- Failover policy information
- Cluster hardware configuration

For well-designed applications, failover for both planned and unplanned outages occurs in seconds.

Product Availability

How is Oracle Fail Safe 2.1 packaged and distributed?

The Oracle Fail Safe 2.1 production CD supports Oracle8 release 8.0.4 and Oracle7 releases 7.3.3 and 7.3.4.

What additional software and hardware are required for Oracle Fail Safe 2.1?

- Oracle Enterprise Manager Version 1.5
- Windows NT 4.0 Enterprise Edition with Service

  Pack 3, and Microsoft Cluster Server (MSCS)
- A Microsoft validated cluster configuration

Further Information

Where can I find more information?

- Oracle Fail Safe Product Data Sheet
- Oracle Fail Safe white papers
- Oracle Fail Safe Concepts and Administration Guide
- Oracle Fail Safe Manager online help and tutorial
- Oracle Fail Safe Quick Tour

Also, please visit the “Oracle for Windows NT Clusters” site at http://www.oracle.com/ and click on Clustering Solutions.

Oracle Corporation World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
650.506.7000
800.633.0583
Fax 650.506.7200

International Inquiries:
44.932.872.020
Telex 851.927444(ORACLEG)
Fax 44.932.874.625
http://www.oracle.com/